Increasing the Secrecy Gap in Quasi-Static Rayleigh Channels with Secret Splitting

Chrysanthi Paschou*, Oliver Johnson†, Angela Doufexi*, Ziming Zhu‡, Woon Hau Chin‡.
*Department of Electrical & Electronic Engineering, University of Bristol, UK † School of Mathematics, University of Bristol, UK
‡Bristol Research & Innovation Laboratory, Toshiba Europe Limited, U.K.
e-mail: chrysanthi.paschou@bristol.ac.uk

***Abstract*—To secure transmissions in the presence of a passive eavesdropper whose Channel State Information (CSI) is unknown, classical Physical Layer Security (PLS) uses Artificial Noise (AN) in order to degrade the eavesdropper's channel. This paper suggests an alternative way of achieving confidentiality which is based on Base Station (BS) cooperation on the downlink as supported in 3GPP LTE-advanced and future 5G networks. Each BS sends a sequence to the legitimate receiver who is able to reconstruct the information message by XoR-ing the received sequences. As long as the eavesdropper(s) is not at the same location as the legitimate receiver, there is a likelihood that one of the links will not be of high quality and, as such, she will not be able to acquire all sequences required for decoding the message. The proposed scheme has low complexity at the receiver and can be used in systems with finite-alphabet input, whereby most Artificial-Noise (AN) based schemes are ineffective.**

***Index Terms*—physical layer security, wiretap coding, base station cooperation, quasi-static Rayleigh channel, reverse training, maximal-ratio transmit beamforming.**

I. Introduction

A. Introduction to PLS

Physical Layer Security (PLS) is a potential realisation of Information Theoretical security which is considered the strictest notion of security. Information Theoretical security is not a new concept; It was introduced by Shannon in 1949 [13] and was revisited by Wyner in 1975 [14] who was the first to see that noise and imperfections in the physical link can be exploited in order to 'hide' information without the need of keys. The main advantages of PLS is that it makes no assumptions on the computational power of the adversary and that its performance can be quantified precisely.

The secrecy coding that PLS uses for confidentiality is called *wiretap coding*. The most popular codes for secrecy purposes are the low-density-parity-check codes, polar codes, and lattice codes [6]. Randomisation among multiple codewords is the key property of wiretap coding and the main difference from the error correcting codes that solely aim for reliability. The randomisation is added in order to confuse the eavesdropper, thereby achieving confidentiality. The redundant bits that aim to confuse the eavesdropper are called the equivocation bits. Notation R_E and R_B refer to the equivocation rate and transmission rate, respectively, and they are measured in bits per second (bps).

This work was supported by the Engineering and Physical Sciences Research Council grant number EP/I028153/1 and Toshiba Europe Limited.

Let C_B be the channel capacity of the legitimate channel and let C_E be the channel capacity of the *wiretap channel*: the channel between the transmitter and the eavesdropper. The difference $C_B - C_E$ is known as the *secrecy gap* and secure transmission via wiretap coding is possible if and only if the secrecy gap is strictly positive. When the transmitter has perfect knowledge of both C_B and $C_E < C_B$, a wiretap code is determined by the doublet (R_B, R_E) such that $R_B \leq C_B$ and $R_E > C_E$. The difference $R_S := R_B - R_E$ defines the *secrecy rate* and expresses how many bits can be sent both reliably and securely per second. The maximum achievable secrecy rate, denoted by C_S, is equal to $C_S := \max(0, C_B - C_E)$.

For many years after Wyner's paper [14], the security community doubted the practicality of PLS due to the restrictive requirement of a strictly positive secrecy gap [11] and the industry had little or no interest in PLS. In the last decade, PLS regained attention. Advancements in wireless technologies such as the employment of multiple-antenna systems can be used in a way that the secrecy gap is increased. The quality of the legitimate channel can be increased by exploiting spatial diversities and mutliplexing gains, whereas the generation of artificial noise can degrade the eavesdropper's channel without effecting the legitimate receiver to the same degree.

The use of artificial noise was introduced by Goel and Negi in 2005 [10] and many AN-based schemes followed since. Most AN-based schemes are often based on the assumption of Gaussian-input signalling and they are not effective in current transmission schemes such as phase shift keying and quadrature amplitude modulation. Some works on AN generation that consider finite inputs exist but they require knowledge of the eavesdropper's CSI. A detailed overview on AN-based schemes that examines theoretical and practical limitations can be found in [3].

B. Inspiration and Our Approach

The scheme aims to provide a positive secrecy gap by degrading the eavesdropper's channel without the use of AN and therefore be applicable in communication systems with discrete-alphabet inputs. We show that the employment of multiple BSs along with an encoding scheme: *secret splitting*

can significantly increase the probability of a positive secrecy gap and allow secure transmissions.

The main idea of the scheme, *secret splitting* (also known as *secret sharing*), has its origins in *network coding* whereby the confidential message is split into M 'splits' and are sent to the legitimate receiver through different paths. In Capar's work [1], [2], a large network of trusted relay nodes is considered and the splits (or shares) travel through parallel paths after appropriate relaying in a multi-hop networks. Loosely speaking, by parallel paths it is meant that the transmission links do not cross at any other location but only at the legitimate receiver. As such, the eavesdropper(s) will not acquire all 'splits' and will fail to decode the message.

Motivated by recent advancements in distributed massive-MIMO and BS corporation, the work examines secret splitting under links created solely in the physical layer. In contrast to secret splitting in network coding, we do not examine the choice of paths/routes for which secrecy is guaranteed. Communications happen in a one-hop manner, the number of BSs is fixed as well as their location. As such, the paths may not be parallel in the sense that the secret splits may travel via beams that overlap. Lastly, our analysis revolves around a single realisation of the fading channel coefficients, and as such it takes no advantage of the fading properties of the channel [5].

C. Organisation

Section II defines and explains secret splitting and secrecy gap under secret splitting. In Section III, the probability of a positive secrecy gap is derived and analysed under a specific channel setting and transmission scheme. A comparison between conventional wiretap coding and secret splitting follows in Section IV and numerical results are presented. The paper concludes with a discussion and future directions in Section V.

D. Notation

Throughout this paper, bold capital letters denote matrices and bold lower case letters denote vectors. The all zero/unit matrix of size $N \times N$ is denoted by $\mathbf{0}_N$/$\mathbf{I}_N$. Notation $i \in [M]$ means that variable i is an element of the set $\{1, 2, \ldots, M\}$. To indicate that x/$\mathbf{x}$ is a standard complex random variable/vector, we write $x \sim \mathcal{CN}(0,1)$ / $\mathbf{x} \sim \mathcal{CN}(\mathbf{0}, I)$. Expression $x \sim \Gamma(k, \theta)$ indicates that random variable x follows the Gamma distribution with shape parameter k and scale parameter θ. The upper upper/lower incomplete gamma function is denoted by $\Gamma_{\text{inc}}(\cdot,\cdot)$/$\gamma_{\text{inc}}(\cdot,\cdot)$. The argument of a complex number is denoted by $|\cdot|$, whereas $||\cdot||$ is used for the Frobenius norm. Lastly, function $H(\cdot)$ is Shannon's entropy, $I(\cdot;\cdot)$ is the mutual information of two variables, and all logarithmic functions are to base two.

II. Secrecy Gap under Secret splitting

A. Secret Splitting

Let $\mathbf{w}$ denote the confidential binary message of length k that Alice wishes to send to Bob in the presence of an eavesdropper, Eve. Alice is able to control M base stations, namely $A_1, A_2, \ldots, A_M$. Alternatively, A_i can also be considered to be a relay node with which Alice can communicate through a secure network.

The transmitter generates $M-1$ uniform independent binary sequences of length k, namely, $\mathbf{w_1}, \ldots, \mathbf{w_{M-1}}$. An M^{th} sequence is generated as

$$\mathbf{w}_M = \bigoplus_{i=1}^{M-1} \mathbf{w_i} \oplus \mathbf{w}. \tag{1}$$

We call $\{\mathbf{w}_i,\ i \in [M]\}$ the *secret splits* of $\mathbf{w}$. Secret split $\mathbf{w}_i$ is sent to Bob through base station A_i. After collecting all M secret splits, Bob XoRs the sequences and attains the confidential message. Indeed, it is evident from (1) that $\bigoplus_{i=1}^{M} \mathbf{w_i} = \mathbf{w}$.

Note that the confidential message $\mathbf{w}$ may not have a uniform distribution, e.g. it may correspond to an English word or to a user's predictable password. However, when random sequence $\bigoplus_{i=1}^{M-1} \mathbf{w_i}$ is XoRed to $\mathbf{w}$, the resulting split, $\mathbf{w}_M$, is also random and independent of $\mathbf{w}$. *Secret splitting* can also be thought as a *one-time pad* encryption [13] with $\bigoplus_{i=1}^{M-1} \mathbf{w}_i$ being the secret key and $\mathbf{w}_M$ being the codeword.

Theorem 1. *As long as the eavesdropper attains less than M secret splits, she gains no information about the confidential message $\mathbf{w}$:*

$$I(\boldsymbol{w}; \mathcal{W}_s) = 0 \quad \textit{for all } \mathcal{W}_s \subset \{\mathbf{w}_i, i \in [M]\}. \tag{2}$$

In Information Theoretical terms, when Eq. (2) is satisfied, *strong secrecy* is achieved which guarantees zero information leakage regardless the length, k, of the message. That is, it only takes one weak link between the eavesdropper and a base station in order to achieve confidentiality.

B. Secrecy Gap

With appropriate wiretap coding, secret split $\mathbf{w}_i$ can be securely transmitted as long as $C_{B_i} - C_{E_i} > 0$. As Th. 1 implies, the secure transmission of one secret split is sufficient for securing message $\mathbf{w}$. Thus, for secrecy purposes, it is required that $C_{B_i} - C_{E_i} > 0$ for some $i \in [M]$. The latter is equivalent to requiring $\max_{i\in[M]}(C_{B_i} - C_{E_i}) > 0$ which motivates the following definition.

Definition 1. The secrecy gap under *secret splitting* is defined as

$$\text{SG}_{\textit{split}} := \max_{i\in[M]} (C_{B_i} - C_{E_i}) \tag{3}$$

When the secrecy gap $\text{SG}_{\textit{split}}$ is positive with probability equal to one or zero, secure communication is possible, or not possible, respectively. When the channels are not deterministic but random processes, quantity $P\left(\text{SG}_{\textit{split}} > 0\right)$ can take any value in the interval $[0, 1]$. The next section studies the probability of a positive secrecy gap under Quasi-Static Rayleigh channel and transmit beamforming.

III. Secrecy Gap in Quasi-Static Rayleigh Channels

A. Channel Model

In our channel model, the legitimate receiver is a single-antenna device, whereas the adversary and transmitter may have multiple antennas. We denote by N_E and N_A the number of antennas at Eve and A_i, respectively. The base stations have the same number of antennas (N_A) for simplicity.

Vector $\mathbf{h}_i = (h_1^{(i)}, \dots h_{N_A}^{(i)}) \in \mathcal{C}^{1\times N_A}$, $i \in [M]$ comprises the channel coefficients $h_j^{(i)}$ of the channel between the j^{th} antenna of A_i and Bob. The matrix $\mathbf{G}_i = (\mathbf{g}_1^{(i)}, \dots, \mathbf{g}_{N_A}^{(i)}) \in \mathcal{C}^{N_E\times N_A}$ indicates the channel between Eve and base station A_i. Column $\mathbf{g}_j^{(i)}$ is the channel vector between base station A_i and the j^{th} antenna at Eve. All channels are assumed to be reciprocal, i.e., communication takes place in a time-division-duplex manner.

Bob's and Eve's channels are independent and drawn from a Rayleigh distribution:

$$\mathbf{h}_i \sim \mathcal{CN}(\mathbf{0}_{N_A}, \sigma_{B_i}^2 \mathbf{I}_{N_A}) \text{ and } \mathbf{g}_j^{(i)} \sim \mathcal{CN}(\mathbf{0}_{N_E}, \sigma_{E_i}^2 \mathbf{I}_{N_E}), \tag{4}$$

for all $i \in [M]$ and $j \in [N_E]$.

When base station A_i transmits $\mathbf{x} \in \mathbb{C}^{N_A\times 1}$, the received signal at Bob and Eve are given by

$$y = \mathbf{h}_i\mathbf{x} + n_B^{(i)} \quad \text{and} \quad \mathbf{z} = \mathbf{G}_i\mathbf{x} + \mathbf{n}_E^{(i)}, \tag{5}$$

respectively. Variables $n_B^{(i)}$ and $\mathbf{n}_E^{(i)}$ denote additive white Gaussian noise of zero mean and unit variance/covariance-matrix that vary independently for different $i \in [M]$ and from the transmission of one symbol to the other:

$$n_B^{(i)} \sim \mathcal{CN}(0,1) \quad \text{and} \quad \mathbf{n}_E^{(i)} \sim \mathcal{CN}(\mathbf{0}_{N_E}, \mathbf{I}_{N_E}). \tag{6}$$

B. Transmission scheme

1) Wiretap Coding and modulation: With Bob being a single-antenna node, the base stations transmit the secret splits successively. Before transmission, reliability and equivocation bits may be added to each one of the secret splits resulting in longer binary words. Modulation such as QAM or PSK modulation maps the binary words to a sequence of signals ready for transmission through the medium.

For example, after wiretap coding, secret split $\mathbf{w}_1$ is transmitted as $\mathbf{s}_1 = (s_1, \dots, s_n) \in \mathbb{C}^{1\times n}$ for some $n \in \mathbb{N}$. Note that the length n may differ at other BSs depending on the wiretap coding and modulation scheme used. Without loss for generality, the signal power is normalised to one: $\mathbb{E}(|s_j|^2) = 1$.

2) Transmit beamforming: Transmit beamforming is preferred for secrecy purposes since it avoids CSI leakage at the eavesdropper [7]–[9]. Being unaware of her own channel, the eavesdropper is unable to increase her decoding capabilities, e.g. by performing receive-beamforming. No CSI of the wiretap channel is available at Alice, either. For example, this is the case when the eavesdropper is passive and remains silent. Under this scenario, the best transmit beamforming strategy for secrecy purposes is Maximal-Ratio-Transmit (MRT) beamforming [4, Corr. 2]; With MRT the signal is sent towards the channel direction of the legitimate receiver and, as such, his SNR is maximised.

With the channel remaining static throughout the transmission of a secret split, the MRT beamforming vector $\mathbf{h}_1^H/||\mathbf{h}_1||$ is applied to every symbol of $\mathbf{s}_i = (s_1, \dots, s_n)$. To avoid a complicated notation, we drop the subscript at the symbols. When A_i transmits

$$\mathbf{x} = \frac{\mathbf{h}_i^H}{||\mathbf{h}_i||} s, \tag{7}$$

substitution in (5) shows that the received signals at Bob and Eve are

$$y_i = ||\mathbf{h}_i|| s + n_B^{(i)} \quad \text{and} \tag{8}$$

$$\mathbf{z}_i = \frac{\mathbf{G}_i\mathbf{h}_i^H}{||\mathbf{h}_i||} s + \mathbf{n}_E^{(i)}, \tag{9}$$

respectively.

C. Probability of positive secrecy gap

Given the unit variance receiver-noise and the normalised to unit power signal, the average SNRs for sequence $\mathbf{s}_i$ at the two receivers are given by

$$\gamma_{B_i} = ||\mathbf{h}_i||^2 \quad \text{and } \gamma_{E_i} = ||\mathbf{G}_i\mathbf{h}_i^H||^2/||\mathbf{h}_i||^2 \tag{10}$$

Theorem 2. *Distribution of SNR at two receivers*

1) Variable γ_{B_i} follows the Gamma distribution with shape parameter N_A and scale parameter $\sigma_{B_i}^2$:

$$\gamma_{B_i} \sim \Gamma(N_A, \sigma_{B_i}^2). \tag{11}$$

2) Variable γ_{E_i} is independent of γ_{Bi} and follows the gamma distribution with shape parameter N_{E_i} and scale parameter $\sigma_{E_i}^2$:

$$\gamma_{E_i} \sim \Gamma(N_E, \sigma_{E_i}^2). \tag{12}$$

3) The expected values of γ_{Bi} and γ_{E_i} are

$$\bar{\gamma_{Bi}} := N_A\sigma_{B_i}^2 \text{ and } \bar{\gamma_{E_i}} = N_E\sigma_{Ei}^2. \tag{13}$$

Observe that Bob's average SNR is a linear function of N_A whilst Eve's average SNR is a linear function of N_E. Only Bob benefits from an increase in the number of antennas at Alice.

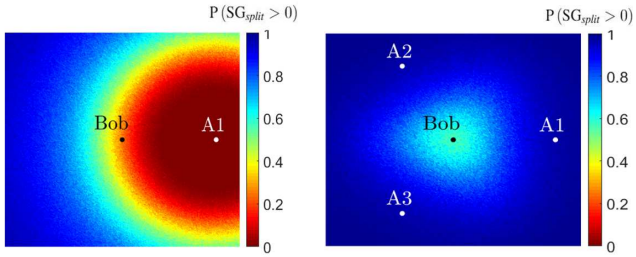
Theorem 3. *The probability of positive secrecy gap under secret splitting is*

$$P\left(SG_{split} > 0\right) = 1 - \prod_{i=1}^{M} P\left(\gamma_{E_i} \geq \gamma_{B_i}\right). \tag{14}$$

Theorem 4. *The probability of positive secrecy gap under secret splitting, MRT, and independent Rayleigh channels is equal to:*

$$P\left(SG_{split} > 0\right) =$$

$$1 - \prod_{i=1}^{M} \int_0^\infty \frac{{\gamma_{B_i}}^{N_A-1} \exp\left(\frac{-\gamma_{B_i}}{\sigma_{B_i}^2}\right) \sum_{k=1}^{N_E-1} \frac{1}{k!} \left(\frac{\gamma_{B_i}}{\sigma_{E_i}^2}\right)^k}{{\sigma_{B_i}}^{2N_A}(N_A-1)!} d\gamma_{B_i} \tag{15}$$



(a) $M = 1, N_A = 1, N_E = 2$ (b) $M = 3, N_A = 1, N_E = 2$

Fig. 1: The red colour indicates areas at which a 2-antenna adversary node has a better signal than Bob with high probability. The blue colour indicates the opposite.

Note that the integration in Eq. (4) is with respect to γ_{Bi}. As such, the probability of $P\left(\text{SG}_{split} > 0\right)$ is a function of the channel statistics, σ^2_{Bi} and σ^2_{Ei}, and the number of antennas, N_A and N_E.

Corollary 4.1. *When Eve is a single antenna node ($N_E = 1$), Eq.* (15) *can be expressed as*

$$P\left(SG_{split} > 0\right) = 1 - \prod_{i=1}^{M} \left(1 + \frac{\sigma^2_{B_i}}{\sigma^2_{E_i}}\right)^{-N_A}. \tag{16}$$

From a user's location point of view, by invoking the relationship between average signal power and distance [12], the channel statistics can be expressed as

$$\sigma^2_{Bi} = k/d(A_i, B)^{\alpha} \text{ and } \sigma^2_{Ei} = k/d(A_i, E)^{\alpha}, \tag{17}$$

for some $k \in \mathbb{R}$, where $d(A_i, B)/d(A_i, E)$ is the distance between A_i and Bob/Eve and α is the path-loss exponent. For example, Eq. (16) is equivalent to

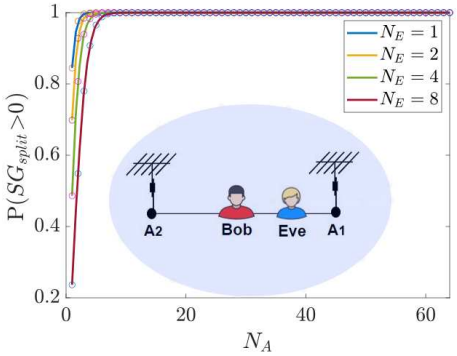
$$P\left(\text{SG}_{split} > 0\right) = 1 - \prod_{i=1}^{M} \left(1 + \left(\frac{d(A_i, E)}{d(A_i, B)}\right)^{\alpha}\right)^{-N_A}. \tag{18}$$

Although the probability of a positive secrecy gap is a function of the path-loss exponent α, the differences in the graphs for different values of $\alpha \in [3, 5]$ were hardly noticeable. All numerical results of this paper consider the case when $\alpha = 4$ only.

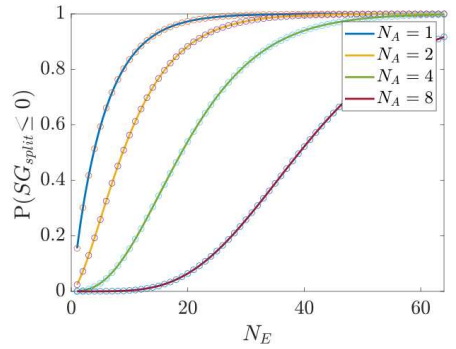
In Figure 1a the red area indicates the locations at which the eavesdropper has an advantage over Bob. i.e., locations at which the probability of a positive gap is low. When three single-antenna BSs (or relay nodes) are employed, the likelihood that Eve attains a better signal than Bob is decreased dramatically (Fig. 1b).

D. Asymptotic behaviour

It is evident from Th. 3 that the probability of positive secrecy gap is an increasing function of the number of base-stations, M; If Eve is equipped with a finite number of antennas then it is a strictly increasing function. In the latter



(a) Probability of positive SG$_{split}$ as an increasing function of N_A.



(b) Probability of non-positive SG$_{split}$ as an increasing function of N_A.

Fig. 2: Probability of positive/negative SG$_{split}$ against N_A/N_E when two BSs are employed ($M = 2$) and Eve is at the middle between Bob and A_1. Solid lines/scattered plots are derived theoretically/empirically.

case, when M becomes asymptotically large, the secrecy gap under secret splitting is positive with probability one:

$$\lim_{M\to\infty} P\left(\text{SG}_{split} > 0\right) = 1. \tag{19}$$

On the other hand, for a fixed number BSs, M, secure communication is not possible when $N_E \to \infty$. Indeed, with an asymptotically large number of antennas available at Eve only, she always experiences a better SNR than Bob. Since $P\left(\gamma_{E_i} \geq \gamma_B\right) = 1$ for all $i \in [M]$, it follows that

$$\lim_{N_E\to\infty} P\left(\text{SG}_{split} \leq 0\right) = 1. \tag{20}$$

Consider the metrics $P\left(\text{SG}_{split} > 0\right)$ and $P\left(\text{SG}_{split} \leq 0\right)$, i.e., the probability of Bob being successful and Eve successful in terms of achieving a better signal, respectively. For the setting as illustrated in Fig. 2a whereby two base stations are deployed, the probability of Bob being successful converges much faster than the probability of Eve being successful. Indeed, even when the adversary is equipped with $N_E = 8$ antennas, ten antennas at each BS is sufficient to provide a positive secrecy gap with probability approximate to one (0.9999). On the other hand, when $N_A = 8$, the eavesdropper

needs at least forty antennas for a 50% chance to get a better signal than the legitimate receiver (Fig. 2b).

Lastly, for the case when $N_A \to \infty$, it is evident from Eq. (11) and (12) that the employment of an infinite number of antennas N_A increases Bob's SNR asymptotically. As such, for a fixed number of antennas at Eve, we have that $P(\gamma_{E_i} \geq \gamma_{Bi}) = 0$ for all $i \in [M]$ which results in a certain positive secrecy gap:

$$\lim_{N_A \to \infty} P(SG > 0) = 1. \tag{21}$$

The above equation implies that the employment of a single base station and conventional wiretap coding are sufficient to secure the communication from Alice to Bob when N_A is asymptotically large.

IV. Base Station Allocation and Numerical Results

A. Secret Splitting Vs Conventional Wiretap Coding

With the probability of positive secrecy gap being an increasing function of both N_A and M, the question arising is whether giving Alice more antennas is more beneficial than employing more BSs for secrecy purposes or vice versa. Besides, when taking into account the transmission rate, a small M is preferred given that Bob is a single antenna device and receives the secret splits successively. Two strategies are considered:

Strg 1: Alice employs $M > 1$ base stations each equipped with K antennas. $(M > 1 \ \& \ N_A = K)$.

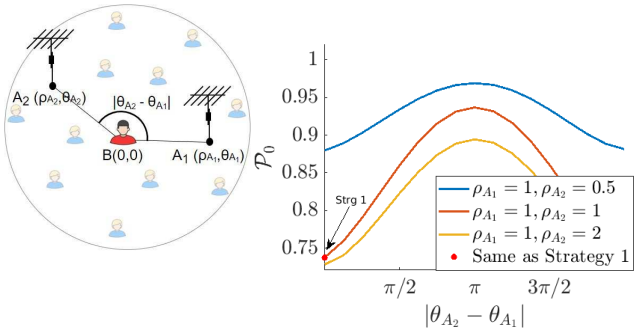
Strg 2: Alice employs one base station with MK antennas. $(M = 1 \ \& \ N_A = MK)$.

The first strategy is referred to as the M-secret splitting strategy, whereas the trivial case $(M = 1)$ is the case of conventional wiretap coding. The total number of antennas is MK for both cases to facilitate comparison. Whether the first strategy outperforms the second in terms of providing a positive secrecy gap depends on the channel statistics of the two receivers. It can be shown that conventional wiretap coding outperforms secret splitting when the eavesdropper channel or location is known at Alice.

When the wiretap CSI is known at Alice, M-secret splitting is unnecessary: Alice can simply transmit with the BS that maximises the ratio $\gamma_{B_i}/\gamma_{E_i} > 1$. Even when only the location of the eavesdropper is known, the trivial case whereby Alice transmits with the BS minimises the ratio of the distances $d(A_i, B)/d(A_i, E)$ maximises the probability of a positive secrecy gap. However, in a practical scenario the location of a passive eavesdropper is unknown. It will be shown, that in the case of a passive eavesdropper, M-secret splitting is a better strategy in terms of secrecy.

With no information on the eavesdropper's location, E, the comparison between the two strategies will be made by evaluating the average performance, $\mathcal{P}_0$, over a set of possible locations for Eve, $\mathcal{E}$:

$$\mathcal{P}_0 := \mathbb{E}[P(\text{SG}_{split} > 0 | E \in \mathcal{E})]. \tag{22}$$



(a) (b)

Fig. 3: The average performance: $\mathcal{P}_0 = \mathbb{E}[P(\text{SG}_{split} > 0 | E \in \mathcal{E})]$ against the angle difference of the two BSs $|\theta_{A_1} - \theta_{A_2}|$ (3b). The set of possible locations for Eve is $\mathcal{E} = C(B, 1.5\rho_{A_1})$ (3a).

The set of possible locations, $\mathcal{E}$, is taken to be either the interior of a square or the interior of a circle:

- $\mathcal{E} = C(B, \rho_E)$: the interior of the circle of radius ρ_E and centre B, i.e., Bob's location, or
- $\mathcal{E} = S(B, \rho_E)$: the interior of some square of base $2\rho_E$ and centre B.

Due to the infinite cardinality of the sets and the complexity of the formulae, the evaluation of the performance $\mathcal{P}_0$ will be derived empirically by sampling the eavesdropper's location in $\mathcal{E}$ uniformly. Note that in this paper Eve and Bob lie on the same plane. The simulation methods have been validated a priori by considering discrete sets of small cardinality for which the theoretical results matched the empirical ones.

The BS allocation plays a critical role in the performance. The following theorem considers the extreme case when all BSs are placed at the same location.

Theorem 5. *When the secret splits are sent from the same location, conventional wiretap coding and secret splitting perform the same in terms of increasing* $\mathcal{P}_0$.

Remark 5.1. Theorem 5 justifies the reason for employing multiple BSs rather than grouping the antennas within a single BS; Splitting a message between groups of antennas at a single BS is equivalent in performance to conventional wiretap coding, so this scheme uses spatially separated BSs.

With Bob being at the origin, $B(0,0)$, of a polar coordinate system, let A_i be placed at $A_i(\rho_{A_i}, \theta_{A_i})$. As Fig. 3b demonstrates, the average performance under 2-secret splitting increases as the difference of the angles of the two base stations approaches π. The angle difference of $|\theta_{A_2} - \theta_{A_1}| = \pi$ will be referred to as the optimal angle-difference. Observe that a near-optimal angle-difference (e.g., $\pi \pm \pi/4$) achieves performances near to the maximum. This is an encouraging result for real-life communication systems when considering that the angle difference will most likely differ from the optimal.

The performance of conventional wiretap coding can also be extracted from the graph in Fig. 3b; According to Th. 5, one simply needs to look at the corresponding value of $|\theta_{A_1} - \theta_{A_2}| = 0$ for the case when $\rho_{A_1} = 1, \rho_{A_2} = 1$. For example, when $\mathcal{E} = C(0, 1.5)$ and $N_E = 1$ Strategy 1 achieves a positive secrecy gap with probability $\mathcal{P}_0 = 0.73$. As for the second strategy, even when A_2 is placed at double the distance from Bob than A_1 ($\rho_{A_2} = 2$), the probability, $\mathcal{P}_0$, increases remarkably (up to 27%).

Table I lists five examples for a set of different parameters. The average performance has been evaluated over the circle $C(B, 1.5\rho_{A_1})$. For the case when $M = 2$, the second base station is placed at distance $\rho_{A_2} = \rho_{A_1} = 1$ from Bob as illustrated in Fig. 3a. Column 'optimal' lists the average performance, $\mathcal{P}_0$, when the BSs are placed diametrically opposed to Bob ($|\theta_{A_2} - \theta_{A_1}| = \pi$). The average performance is also recorded for the case when the angle-difference differs far from the optimal: $|\theta_{A_1} - \theta_{A_2}| = 2\pi/3$. For all cases, Strategy 1 is the best strategy in terms of providing a positive secrecy gap.

TABLE I:
Average Performance $\mathcal{P}_0 = P\left(\text{SG}_{split} > 0 | E \in \mathcal{E}\right)$ under Strategy 1 and Strategy 2. Bob is at the origin $B(0,0)$ and the set of possible locations for Eve is the circle $C(B, 1.5)$. Two cases are considered in Strategy 1: (a) the two BSs are at $A_1(1,0)$ and $A_2(1,\pi)$ forming an 'optimal' angle with Bob (b) the two BSs are at $A_1(1,0)$ and $A_2(1,3\pi/4)$ forming a 'non-optimal' angle.

$\mathcal{P}_0$	**Strategy 1: 2 BSs with K antennas each**		**Strategy 2: 1 BS with 2K antennas**
	optimal	**non-optimal**	
$\mathbf{K = 2, \quad N_E = 1}$	0.981	0.992	0.815
$\mathbf{K = 3, \quad N_E = 1}$	0.999	0.995	0.846
$\mathbf{K = 32, \quad N_E = 1}$	1.00	1.00	0.950
$\mathbf{K = 2, \quad N_E = 64}$	0.098	0.097	0.084
$\mathbf{K = 32, N_E = 64}$	0.950	0.894	0.595

Observe that even when Eve is a single-antenna node, beamforming with $2K = 64$ antennas at one BS does not guarantee a positive secrecy gap ($\mathcal{P}_0 = .95$). On the other hand, distributing the antennas in two BSs (case $K = 32$, $N_E = 1$) results in a positive secrecy gap with probability one. Simulations suggest that when the eavesdropper is a single-antenna node, two BSs with just three antennas each can almost certainly provide the legitimate pair with a positive secrecy gap (case $K = 2, N_E = 1$). Lastly, both strategies perform poorly when the adversary has a much bigger number of antennas than Alice (case $K = 2, N_E = 64$).

B. $M = 2$ Vs $M > 2$

It has been shown that security can significantly be enhanced by distributing the antennas at two base stations when there is no knowledge of the wiretap channel. This section examines the case of multiple BSs ($M \geq 2$) and compares non-trivial secret-splitting strategies when the total number of antennas is fixed for the two cases. I.e., having established

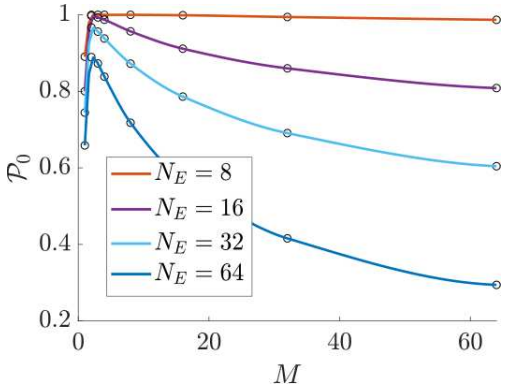


Fig. 4: Average performance: $\mathcal{P}_0 = \mathbb{E}[P\left(\text{SG}_{split} > 0 | E \in \mathcal{E}\right)]$ against the number of BSs (M) when the total number of antennas is fixed to $\sum N_A = 64$. The set of the eavesdropper's possible locations is the square $S(B, 1.5)$ and for every M, the BSs are placed optimally at distance one from Bob.

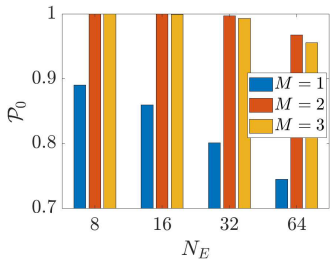


Fig. 5: A closer look at the data of Fig. 4 for the cases where $M \leq 3$ BSs are employed. The performance, $\mathcal{P}_0$, is plotted against the number of antennas at the eavesdropper.

that under an appropriate base station allocation secret splitting outperforms conventional wiretap coding for secrecy, we now examine what is the optimal number of BSs. For example, Alice is concerned whether three BSs with two antennas each perform better than two BSs with three antennas each. The multiple BSs are placed in a way such that they form a regular polygon with Bob being at the centre:

$$A_i \text{ is placed at } (1, 2\pi(i-1)/M). \tag{23}$$

For example, when $M = 3$, the BSs form an equilateral triangle. Assuming that the BSs can have a minimum distance of one from Bob, the above BS allocation is the optimal in terms of increasing the probability $\mathcal{P}_0$. Indeed, by separating the BSs as far as possible form each other whilst the distance between each of them and Bob is kept the minimum, there is always one BS for which Bob is closer to than Eve. As such, the probability of Eve 'missing' a secret split is maximised.

As seen in Figure 4, when the total number of antennas is fixed, the performance is maximised for $M = 2$ and degrades gradually with $M > 2$. In particular, the more antennas employed at Eve, the faster the performance of $\mathcal{P}_0$ degrades with $M > 2$. Therefore, if there exist two BSs that are placed diametrically opposed to Bob, transmitting two splits with two

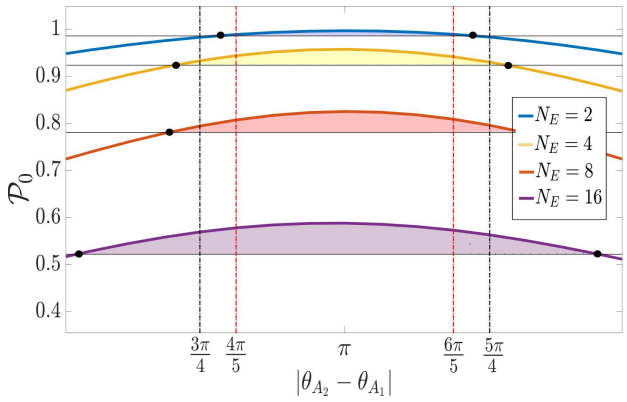


Fig. 6: The curved lines indicate the performance $\mathcal{P}_0$ against the optimal and sub-optimal angle-difference between two BSs. The vertical lines correspond to the case when $M = 3$ are placed optimally. The highlighted segments indicate the angle-differences for which 2 BSs outperform the employment of 3 BSs.

3-antenna BSs is a better strategy than transmitting three splits with three 2-antenna BSs.

Extracting the data from Fig. 4, for $M \leq 3$, Fig. 5 is plotted. Since the difference in the performance of the cases $M = 2$ and $M = 3$ is very small, transmitting with three splits may be more beneficial if the two BSs are not placed optimally. Simulations suggest that $M = 2$ is the optimal number of BSs as long as the angle-difference doesn't differ more than $\pi/5$ from the optimal angle-difference (π). The simulations were run for a different set of parameters: $\sum N_A = 6, 12, 60, 120$ and $N_E \in [10 \sum N_A]$. Figure 6 is an example of the performance for the two cases $M = 2$ Vs $M = 3$ when $\sum N_A = 6$. The curved lines indicate the performance of the case $M = 2$ against the angle-difference whilst the vertical lines indicate the maximum performance for the case $M = 3$. In most cases, the case $M = 2$ performs better even when $3\pi/4 < |\theta_{A_2} - \theta_{A_1}| < 5\pi/4$.

V. Conclusion

In Section II the secret splitting scheme has been explained. The definitions displayed are generic and can be applied in any channel model. Section III has examined our scheme for the case of Rayleigh channels and transmit beamforming. The formulae derived allowed a theoretical analysis and facilitated the numerical results in the following section. Section IV has also demonstrated the importance of base station allocation and has made comparisons between our scheme and conventional wiretap coding in terms of increasing the probability of secrecy gap. It has been shown that under a constraint of the total number of antennas: $\sum N_A \leq K$, it is more beneficial to distribute K antennas among a small number of BSs with two being the optimal number of BSs as long as the legitimate receiver is in between the two BSs. For example, when the legitimate receiver moves along streets or railways, the proposed scheme could find a good fit.

It has been shown that secret splitting can significantly decrease the areas at which the eavesdropper has an advantage over the intended receiver. However, a relatively small secrecy gap may result in impractically long codewords and transmission rates that do not meet the Quality-of-Service requirements. In future work, rates for wiretap coding under secret splitting can be fixed. In scenarios where a target equivocation rate is not met, the information leakage towards the eavesdropper should be quantified. Moreover, the case of a multiple-antenna receiver is also an interesting case; Allowing Bob to receive the secret splits simultaneously will significantly increase the transmission rate whilst benefiting from the security enhancement of secret splitting.

References

[1] Ç. Çapar and D. Goeckel. Network coding for facilitating secrecy in large wireless networks. In *2012 46th Annual Conference on Information Sciences and Systems (CISS)*, pages 1–6. IEEE, 2012.

[2] Ç. Çapar, D. Goeckel, B. Liu, and D. Towsley. Secret communication in large wireless networks without eavesdropper location information. In *2012 Proceedings IEEE INFOCOM*, pages 1152–1160. IEEE, 2012.

[3] K. Cumanan, H. Xing, P. Xu, G. Zheng, X. Dai, A. Nallanathan, Z. Ding, and G. K. Karagiannidis. Physical layer security jamming: Theoretical limits and practical designs in wireless networks. *IEEE Access*, 5:3603–3611, 2016.

[4] S. Gerbracht, C. Scheunert, and E. A. Jorswieck. Secrecy outage in MISO systems with partial channel information. *IEEE Transactions on Information Forensics and Security*, 7(2):704–716, 2011.

[5] S. Goel and R. Negi. Guaranteeing secrecy using artificial noise. *IEEE transactions on wireless communications*, 7(6):2180–2189, 2008.

[6] W. K. Harrison, J. Almeida, M. R. Bloch, S. W. McLaughlin, and J. Barros. Coding for secrecy: An overview of error-control coding techniques for physical-layer security. *IEEE Signal Processing Magazine*, 30(5):41–50, 2013.

[7] P.-C. Lan, Y.-W. P. Hong, and C.-C. J. Kuo. Enhancing secrecy in fading wiretap channels with only transmitter-side channel state information. In *2014 IEEE Globecom Workshops (GC Wkshps)*, pages 1314–1319. IEEE, 2014.

[8] T.-Y. Liu, P.-H. Lin, S.-C. Lin, Y.-W. P. Hong, and E. A. Jorswieck. To avoid or not to avoid CSI leakage in physical layer secret communication systems. *IEEE Communications Magazine*, 53(12):19–25, 2015.

[9] T.-Y. Liu, S.-C. Lin, and Y.-W. P. Hong. On the role of artificial noise in training and data transmission for secret communications. *IEEE Transactions on Information Forensics and Security*, 12(3):516–531, 2016.

[10] R. Negi and S. Goel. Secret communication using artificial noise. In *IEEE Vehicular Technology Conference*, volume 62, page 1906. Citeseer, 2005.

[11] H. V. Poor and R. F. Schaefer. Wireless physical layer security. *Proceedings of the National Academy of Sciences*, 114(1):19–26, 2017.

[12] T. S. Rappaport. Wireless communications–principles and practice. *Microwave Journal*, 45(12):128–129, 2002.

[13] C. E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656–715, 1949.

[14] A. D. Wyner. The wire-tap channel. *Bell System Technical Journal*, 54(8):1355–1387, 1975.